IN THE CLAIMS:

The following is a current listing of claims and will replace all prior versions and listings of claims in the application. Please amend the claims as follows:

1–104. (Canceled)

105. (Currently Amended) A computer-implemented method comprising:

selecting an active program on a computer system as code under investigation, wherein the program is running on the computer system in a manner that permits the program to infect the computer system; and

successively executing ~~malicious code detection code (MCDC) on the computer system, wherein the MCDC includes~~ each of a first and a second plurality of detection routines, wherein said executing includes:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results; and

weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation has characteristics and/or behaviors typically associated with valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results;

weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation has characteristics and/or behaviors typically associated with malicious code, wherein the second score is obtained independently of the first score; and

upon completing the executing of the first and second plurality of detection routines, using the first and/or second scores to categorize the code under investigation with respect to the likelihood of the code under investigation compromising the security of the computer system.

106. (Canceled)

107. (Currently Amended) The method of claim 105, further comprising:

selecting, in turn, each of a plurality of additional active programs on the computer system as code under investigation, wherein each of the plurality of additional active programs is running on the computer system in a manner that permits infection of the computer system; and

successively executing ~~said MCDC~~ each of the first and second plurality of detection routines with respect to said selected code under investigation.

108. (Canceled)

109. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect remote control software.

110. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect a keystroke logger.

111. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect spyware.

112. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect a worm.

113. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect a virus.

114. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect monitoring software.

115. (Currently Amended) A computer-implemented method comprising:

selecting code currently running on a computer system as code under investigation, wherein said code is running in a manner that permits infection of said computer system; and

executing, in turn, ~~malicious code detection code (MCDC) on the computer system, wherein the MCDC includes~~ each of a first and a second plurality of detection routines on the computer system, wherein said executing includes:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results;

weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation has characteristics and/or behaviors typically associated with valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results; and

weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation has characteristics and/or behaviors typically associated with malicious code, wherein the second score is independent of the first score; and

upon executing each of the first and second plurality of detection routines:

using the first and/or second scores to categorize the code under investigation into one of a plurality of categories, including first and second categories indicative of valid code and malicious code, respectively.

116. (Canceled)

117. (Previously Presented) The method of claim 115, wherein at least some of the code associated with the selected active code is running in kernel mode.

118. (Currently Amended) The method of claim 115, further comprising:

selecting additional active code as code under investigation; and

executing each of the first and second pluralities of detection routing ~~said MCDC~~ with respect to

said selected code under investigation.

119-126. (Canceled)

127. (Currently Amended) A computer system comprising:

a processor; and

a memory storing program instructions executable by the processor to:

select a program currently running on a computer system as code under investigation, wherein said program is running in a manner that permits infection of said computer system; and

successively execute each of ~~malicious code detection code (MCDC) on the computer system, wherein the MCDC includes~~ a first and a second plurality of detection routines on the computer system, including:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results;

weighting each of the first plurality of results to obtain a first score indicative of the extent to which the code under investigation has characteristics and/or behaviors typically associated with valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results; and

weighting each of the second plurality of results to obtain a second score indicative of the extent to which the code under investigation has characteristics and/or behaviors typically associated with malicious code; and

upon completing execution of the first and second plurality of detection routines, use[[ing]] the first and/or second scores to make a determination ~~determine~~ whether the code under investigation represents a security threat to the computer system.

128. (Currently Amended) A computer-readable memory medium, including program instructions that are computer executable by a computer system to:

select a program currently running on the computer system as code under investigation, wherein said program is running in a manner that permits infection of said computer system; and

successively execute each of ~~malicious code detection code (MCDC) on the computer system, wherein the MCDC includes~~ a first and a second plurality of detection routines on the computer system, ~~and wherein execution of the MCDC~~ include[[es]]ing:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results, wherein the first plurality of detection routines test for characteristics and/or behaviors typically associated with valid code;

weighting and combining each of the first plurality of results to obtain a first composite score;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results, wherein the first plurality of detection routines test for characteristics and/or behaviors typically associated with malicious code; and

weighting and combining each of the second plurality of results to obtain a second composite score; and

upon executing each of the first and second plurality of detection routines, use[[ing]] the first and/or second composite scores to make a determination ~~determine~~ whether the code under investigation is malicious code.

129. (Previously Presented) The method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is malicious code.

130. (Previously Presented) The method of claim 129, wherein the malicious code does not have a known signature.

131. (Previously Presented) The method of claim 105, wherein the first plurality of detection routines includes routines that examine the behavior of the code under investigation.

132. (Previously Presented) The method of claim 131, wherein the second plurality of detection routines includes routines that examine the behavior of the code under investigation.

133. (Previously Presented) The method of claim 105, wherein the malicious code is a previously unknown type of malicious code.

134. (Previously Presented) The method of claim 129, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

135. (Currently Amended) The method of claim 105, wherein the determination is made ~~further comprising~~:

~~determining~~ from the first and second scores that the code under investigation is valid code.

136. (Currently Amended) The method of claim 105~~135~~, wherein the determination is made that the code under investigation is valid code, wherein the determination is made based on the first score exceeding a valid code threshold value and regardless of the second score.

137. (Currently Amended) The method of claim 105, wherein the determination is made that the code under investigation is valid code, wherein the determination is made based on the first score exceeding a valid code threshold and the second score not exceeding a malicious code threshold ~~further comprising:~~

~~determining from the first and second scores that the code under investigation is suspicious code, wherein suspicious code has not been determined to be either valid or malicious code~~.

138. (Currently Amended) The method of claim 105~~137~~, further comprising:

determining from the first and second scores that the code under investigation is suspicious code, wherein suspicious code has not been determined to be either valid or

malicious code ~~wherein the code under investigation is determined to be suspicious code based on the first and second scores being similar~~.

139. (Currently Amended) The system of claim 127, wherein the ~~further comprising~~ program instructions are executable by the processor to:

determine from the first and second scores that the code under investigation is malicious code.

140. (Previously Presented) The system of claim 139, wherein the malicious code is a previously unknown type of malicious code.

141. (Previously Presented) The system of claim 139, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

142. (Currently Amended) The system of claim 127, wherein the ~~further comprising~~ program instructions are executable by the processor to:

determine from the first and second scores that the code under investigation is valid code.

143. (Currently Amended) The system of claim 142, wherein the determination that the code under investigation is valid code is based on the first score exceeding a valid code threshold value and regardless of the second score.

144. (Previously Presented) The system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is suspicious code.

145. (Currently Amended) The memory medium of claim 128, wherein the ~~further comprising~~ program instructions are executable by the computer system to:

determine from the first and second scores that the code under investigation is malicious code.

146. (Previously Presented) The memory medium of claim 145, wherein the malicious code is a previously unknown type of malicious code.

147. (Currently Amended) The memory medium of claim 128, wherein the ~~further comprising~~ program instructions are executable by the computer system to:

determine from the first and second scores that the code under investigation is valid code.

148. (Currently Amended) The memory medium of claim 147, wherein the determination that the code under investigation is valid code is based on the first score exceeding a valid code threshold value and regardless of the second score.

149. (Previously Presented) The memory medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is suspicious code.

150. (Previously Presented) The memory medium of claim 145, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

151. (Previously Presented) The method of claim 105, wherein at least some of the code associated with the selected active program is running in kernel mode.

152. (Currently Amended) One or more computer-readable media storing program instructions executable on a computer system to:

while a first program is running on the computer system in a manner that permits the first program to infect the computer system:

successively execute each of a first and second plurality of detection routines to gather information about the first program, including behavioral information about the first program, wherein the first plurality of detection routines are executable to detect behavior indicative of valid code, and wherein the second plurality of detection routines are executable to detect behavior indicative of malicious code;

upon completing execution of each of the first and second plurality of detection routines:

use the results of the first plurality of detection routines to determine a first value indicative of the likelihood that the first program is valid code ~~characteristics and/or behaviors exhibited by a first program running on the computer system~~;

use the results of the second plurality of detection routines to ~~independently~~ determine a second value indicative of the likelihood that the first program is malicious code ~~characteristics and/or behaviors exhibited by the first program~~;

~~based on comparisons involving~~ use the first and/or second values[[,]] to determine whether the first program is a security threat to the computer system.

153. (Previously Presented) The computer-readable media of claim 152, wherein the program instructions are executable to determine whether the first program is a security threat to the computer system based on a first comparison between the first value and a valid code threshold value and also based on a second comparison between the second value and a malicious code threshold value.

154. (Previously Presented) The computer-readable media of claim 152, wherein the program instructions are executable to determine that the first program is a security threat to the computer system based on the first value not exceeding a valid code threshold value and on the second value exceeding a malicious code threshold value.

155. (Currently Amended) The computer-readable media of claim 152, wherein the program instructions are executable to determine that the first program is not a security threat to the computer system based on the first value exceeding a valid code threshold value and regardless of the second value.

156. (Previously Presented) The computer-readable media of claim 152, wherein the program instructions are executable to determine that the first program is not a security threat to the computer system based on the first value exceeding a valid code threshold value and on the second value not exceeding a malicious code threshold value.

157-158. (Canceled)

159. (Currently Amended) A method, comprising:

while a first program is running on a computer system in a manner that permits the first program to infect the computer system, successively executing each of a first and second plurality of detection routines, wherein the first plurality of detection routines are executable to determine behaviors of the first program that are indicative of valid code, and wherein the second plurality of detection routines are executable to determine behaviors of the first program that are indicative of malicious code;

upon completing the executing of the first and second plurality of detection routines:

using results of the first plurality of detection routines to compute[[ing]] a first score indicative of the likelihood that the first program is valid code ~~characteristics and/or behaviors exhibited by a first program running on a computer system~~;

using results of the second plurality of detection routines to compute[[ing]] a second value indicative of the likelihood that the first program is malicious code ~~characteristics and/or behaviors exhibited by the first program~~;

using the computed first and/or second values to categorize the first program as to the likelihood of the first program compromising the security of the computer system.

160-161. (Canceled)

162. (Previously Presented) The method of claim 159, wherein said using includes performing comparisons involving the first and second values.

163. (Previously Presented) The method of claim 162, wherein said first program is categorized based on a comparison between the first score and a valid code threshold.

164. (Currently Amended) The method of claim 163, wherein the first program is categorized as not being a security threat based on the first score exceeding the valid code threshold and regardless of the second score.

165. (Previously Presented) The method of claim 162, wherein said first program is categorized based on a comparison between the first score and a valid code threshold and also on a comparison between the second score and a malicious code threshold.

166. (Previously Presented) The method of claim 165, wherein the first program is categorized as not being a security threat based on the first score exceeding the valid code threshold and the second score not exceeding the malicious code threshold.

167. (Canceled)